National Webcast Initiative
Cyber Security Risk Assessment Webcast
August 26, 2004
Glossary of Terms

The following definitions are provided as a resource to help familiarize you with some common cyber security terms and phrases you will hear during the August 26, 2004 webcast. The information provided below is by no means an exhaustive list, however it can be utilized as a foundation from which you can build your knowledge of cyber security terms and further pursue these topics on your own.

Term	Definition
Asset	A major application or general support system or logically related groups of systems. Includes hardware, operating systems, databases and communication interfaces. *Examples:* • *Human resources system (including application, database, web self-service portal)* • *Wireless network (including wireless access points, VPN and wireless NICs)*
Asset Value	The value assigned to an asset based on its use within the organization. Value may be expressed in qualitative terms (e.g., high, medium or low); or in quantitative terms (e.g., monetary value or time the system must be available). *Examples:* • *Financial reporting systems would be considered high value for a public company* • *Operational monitoring system for a power station might be valued as 100% required availability*
Impact	The adverse effect resulting from a successful threat exercise of a vulnerability. Can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. *Examples:* • *Loss of internet connectivity due to a denial of service attack from an external hacker* • *Disclosure of sensitive data stored on a laptop stolen from an office*

Term	Definition
Likelihood	The probability that a potential vulnerability may be exercised within the construct of the associated threat environment. Likelihood should be determined after consideration of: • Threat-source motivation and capability • Nature of the vulnerability • Existence and effectiveness of current controls. *Examples:* • *The likelihood that an SQL Injection vulnerability could be exercised by a hacker is medium (on a scale of high, medium, low)* • *The likelihood of an internal user exploiting a weakness in the design of a payroll system is 0.8 (on a scale of 0=low to 1=high)*
Security Controls	(1) Operational controls – address security methods primarily implemented and executed by people. *Examples:* • *Review of access logs to determine failed login attempts* • *Development and implementation of information security policies and procedures* (2) Technical controls – hardware and software controls that provide automated protection to systems or applications. *Examples:* • *Passwords used to authenticate a user prior to granting access to a system* • *Firewall rules that prohibit certain traffic entering a network*
Security Requirements	List of control objectives or standards that must be met in the design of a system. *Examples:* • *Requirements derived from regulations such as HIPAA Security Rule* • *NIST Common Criteria for IT Security*

Term	Definition
Security Risk	Impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur.
Security testing	Techniques used to confirm the design and/or operational effectiveness of security controls implemented within a system. *Examples:* • *Attack and penetration studies to determine whether adequate controls have been implemented to prevent breach of system controls and processes* • *Password strength testing by using tools ("password crackers"). These tools attempt to guess a user's password by encrypting common dictionary terms (and many possible combinations and permutations) and comparing the result with the user's encrypted password*
System owner	The individual responsible for establishing the rules for appropriate use and protection of the data/information within a system. The system owner retains that responsibility even when the data/information are shared with other organizations.
Threat	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability. *Examples:* • *Terminated employees using knowledge gained while employed (e.g., remote access phone numbers) to obtain unauthorized access* • *Hackers identifying and exploiting vulnerabilities in the design of an Internet connection.*
Threat source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability *Examples:* • *Terminated employees* • *Hackers*

Term	Definition
Vulnerability	A flaw or weakness in system security procedures, design or implementation that could be exercised (accidentally triggered or intentionally exploited) and result in a harm to an IT system or activity. *Examples:* • *Terminated employees system identifiers (ID) are not removed from the system* • *Vendor released patches have not been installed*